5V-01

# iOSのVPNサービスを利用したNTMobile実装方式の提案

渡邉 憲士 [†1]　清水 一輝 [†2]　鈴木 秀和 [†2]　内藤 克浩 [†3]　渡邊 晃 [†2]
[†1] 名城大学理工学部　[†2] 名城大学大学院理工学研究科　[†3] 愛知工業大学情報科学科

## 1 はじめに

スマートデバイスの普及に伴い，携帯端末と IP ネットワーク接続装置が，自由に通信できることが望まれている．これを実現するには相手端末が NAT 配下にある場合でも通信を開始することができる NAT 越え通信，および通信中に一方がネットワークを切り替えても通信を継続できる移動透過性が要求される．筆者らはこれらの機能を実現する技術として NTMobile(Network Traversal with Mobility)[1] を提案し，LINUX で動作を検証してきた．本稿では iOS の VPN サービスを利用して，iOS で NTMobile を実現する方法を提案する．

## 2 NTMobile

### 2.1 NTMobile の概要と動作

NTMobile は NAT 越え通信と移動透過性を同時に実現する技術である．図 1 に NTMobile の動作概要を示す．図では NAT を省略してあるが，どのようなネットワーク構成でも通信を確立することができ，通信中に移動しても通信を継続できる．通信を開始する端末を MN，相手端末を CN とする．DC(Direction Coordinator) は仮想 IP アドレスの割り当てと経路の指示を行う．RS(Relay Server) は MN と CN が直接通信できない場合にパケットを中継する装置である．DC，RS はグローバルネットワーク上に設置し，分散配置することができる．

MN が DC に経路指示要求をすると，DC は MN と CN に対して適切なトンネル構築指示を行う．これにより通信経路が決定し，MN/CN 間でトンネル通信を行うことができる．MN または CN がネットワークを切り替えた時は，再度同じ処理を実行し，新しいトンネル経路で通信を行う．仮想 IP アドレスは変化しないので通信を継続できる．NTMobile をアプリケーションとしてインストールすることにより，既存のアプリケーションをそのまま利用することができる．ネットワーク機器や端末のカーネルに変更を加える必要はない．

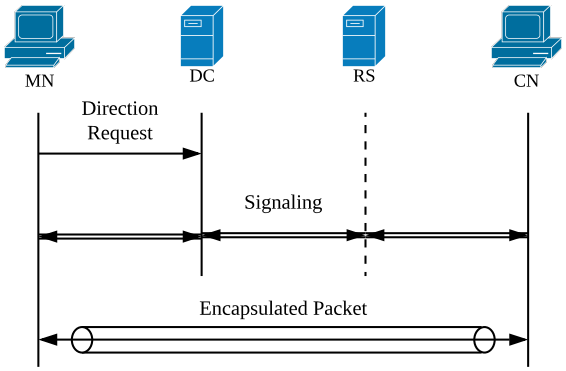


図 1　NTMobile 動作概要

### 2.2 Linux における実現

NTMobile はシグナリング処理とパケット生成処理をアプリケーションレベルで実現し，通信ライブラリとして提供している．この通信ライブラリを NTMobile framework(以下 NTMfw)[2] と呼ぶ．LINUX では TUN サービス上で NTMfw を利用して実現 [3]，既存のアプリケーションをそのまま使えるようにした．TUN とはトンネル通信をアプリケーションで実現することを可能にするサービスである．

図 2 に TUN NTMobile の構成を示す．TUN NTMobile は全て C で記述した．一般アプリケーションは仮想インタフェースとの間でパケットを送受信する．送信時は，TUN NTMobile の Packet Analysis Module がパケットをフックして解析する．フックしたパケットが DNS 問い合わせの場合，Signaling Module にてトンネル構築処理を開始する．トンネル構築処理が完了すると DNS 応答パケットを作成し，仮想インタフェースを経由して相手の仮想 IP アドレスを MN のリゾルバに返信する．フックしたパケットが仮想 IP アドレス宛のパケットであればこれを単にデータとして扱い，Packet Manipulation Module にてデータの暗号化と NTM ヘッダ，MAC の付与を行う．その後，CN の実 IP アドレス宛に UDP ソケットを用いて実インタフェースから送信することにより，トンネル通信を実現する．

---

**Proposal for Realization Method of NTMobile utilizaing iOS VPN**

Kenshi Watanabe[†1], Kazuki Shimizu[†2] Hidekazu Suzuki[†2] Katsuhiro Naito[†3]and Akira Watanabe[†2]
[†1] Faculty of Science and Technology, Meijo University
[†2] Graduate School of Science and Technology, Meijo University
[†3] Faculty of Information Science, Aichi Institute of Technology

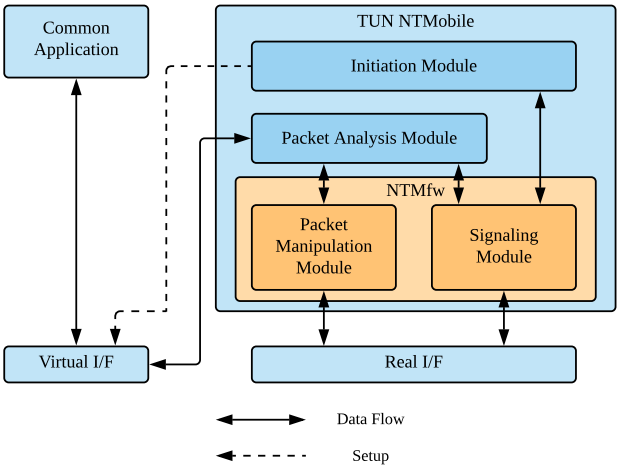


図 2　TUN NTMobile 構成

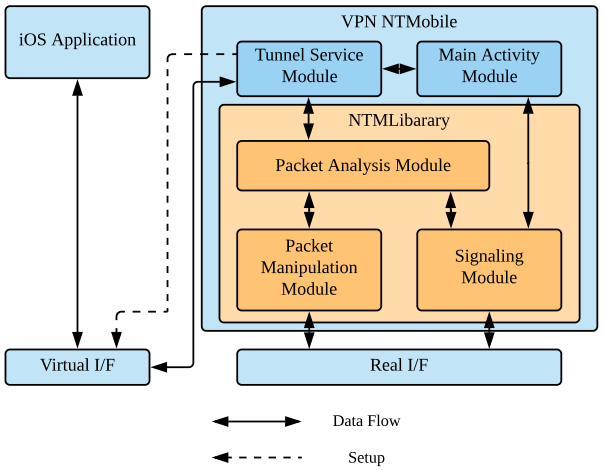


図 3　VPN NTMobile の構成

## 3　iOS における実現方式

### 3.1　NetworkExtension

iOS では TUN インタフェースの代わりに，NetworkExtension フレームワークを利用する．これは Linux の TUN サービスと類似のサービスで，ルート権限を利用することなく iOS にてトンネル通信を実現できる．NetworkExtension フレームワークには iOS のネットワーク機能を拡張する API が複数用意されているが，本提案では NETunnelProviderManager クラスと NEPacketTunnelProvider クラスを利用する．NEtunnelProviderManager クラスは VPN 接続を構成するクラスであり，接続を確立することによって NEPacketTunnelProvider クラスを呼び出すことができる．NEPacketTunnelProvider クラスを継承したサブクラスを作成することによって，そのサブクラスが仮想インタフェースにアクセスできるようになる．

### 3.2　モジュール構成と動作

図 3 に VPN NTMobile の構成を示す．基本的に TUN NTMobile と同様の構成をとることができるため，OS の違いにより異なる部分を切り出し，SWIFT で記述した．SWIFT と C 言語は互換性があり相互に呼び出すことができる．TUN NTMobile の Initiation Module を取り除いた部分ををライブラリとして利用して他の OS でも利用可能にした．このライブラリは Android，Windows でも利用可能である．

アプリケーション起動時に最初に呼び出されるモジュールは SWIFT で記述する必要があるため，Main Activity Module を追加した．これは TUN NTMobile の Initiation Module に対応しており，NTMobile の起動，通信開始，終了処理を行う．起動処理は GUI から NTMobile のアカウント情報を受け取り，Signaling Module にて NTMobile のログイン処理を行う．Main Activity Module だけでは仮想インタフェースの生成ができないため，NTMobile ログイン処理終了後，取得した自らの仮想 IP アドレスを利用して Tunnel Service Module にて仮想インタフェースの生成処理を実行する．GUI から CN の FQDN を入力することで Signaling Module による経路の構築を行い、NTMobile 通信を開始することができる．

次に，iOS では Packet Analysis Module でパケットをフックできないため，Tunnel Service Module を追加した．このモジュールには NEPacketTunnelProvider クラスを継承したサブクラスを作成する．これにより仮想インタフェースにアクセスできるようになり，iOS アプリケーションが送信したパケットをフックできる．フックしたパケットを Packet Analysis Module に渡すことにより，TUN NTMobile と全く同じ処理を行うことができる．

## 4　まとめ

本稿では iOS の VPN サービスを利用して，NTMobile を実現する方式を提案した．現在，提案方式を実装中で今後検証を行っていく予定である．

### 参考文献

[1] 上醉尾一真ほか：IPv4/IPv6 混在環境で移動透過性を実現する NTMobile の実装と評価，情処学論，vol.54，No.10，pp.2288-2299 (2013).
[2] 納堂博史ほか：実用化に向けた NTMobile フレームワークの実装と評価，情処学論，Vol.160，No.1，TBD (2019).
[3] 稲垣智ほか：LAN 内通信システムをインターネット上で利用可能にする TUN アプリの提案と実装，全国大会講演論文集，vol.1，pp215-216 (2018).